Abstract

The fourth generation technology of broadband wireless networks i.e. WiMAX (Worldwide Interoperability for Microwave Access) became popular due to its features like high speed internet access, large coverage area and interoperability for different type of devices. Non-Line of-sight propagation with lower frequency improvement makes WiMAX vulnerable to various security threats. Hence, authentication and authorization are used for protecting network from various attacks. Although there are standard authentication protocols in IEEE 802.16, but still WiMAX is vulnerable to attacks such as replay attack, DoS (denial of service attack), interleaving attack etc. In this paper, an exhaustive analysis of existing solutions in standard PKMv2 (privacy key management version 2) protocol is presented. The Proxy Base Station based authentication protocol addresses the major attacks namely DoS attack, interleaving
attack, replay attack and downgrade attack. With the introduction of PS (proxy base station),
the task of validation is distributed between the PS and BS (base station), it resolves the DoS
attack due to the resource exhausting validation procedure [23]. Our proposed authentication
protocol is modeled and verified on CPN (Colored PetriNet) tool (version 3. 0. 2)[1, 2] with and
without intruder and compared with PKMv2 standard protocol. The state space analysis report
for standard verification parameters shows that our proposed protocol satisfies the desired
properties of liveliness and fairness with negligible overheads and it is secure and efficient.

References

- Al-Azzoni, D. G. Down and R. Khedri, ”Modeling and verification of cryptographic
- WiMAX Forum, Fixed, Nomadic, Portable and Mobile Applications for 802. 16-2004 and
  802. 16e WiMAX (Nov. 2005).
- IEEE 802. 16-2005, IEEE standard for Local and Metropolitan Area Networks- Part 16:
- Anjali Sardana and R. C. Joshi, ”Simulation of Dynamic Honeypot Based
  Redirection to Counter Service Level DDoS Attack,”, Lecture Notes in Computer Science:
- Anjali Sardana, K. Kumar and R. C. Joshi, ”Detection and Honey pot Based
  Redirection to Counter DDoS Attacks in ISP Domain,”, Third International Symposium on
- Anjali Sardana and R. C. Joshi, ”Honeypot Based Routing to Mitigate DDoS
  Attacks on Servers at ISP Level,”, International Symposiums on Information Processing
- Anjali Sardana and R. C. Joshi, ” Autonomous Dynamic Honeypot Routing
  Mechanism For Mitigating DDoS Attacks in DMZ,”, 16th IEEE International Conference on
  Networks (ICON 2008),1-7(2008).
- Anjali Sardana and R. C. Joshi, ”An Auto Responsive Honeypot Architecture For
  Dynamic Resource Allocation and QoS Adaptation in DDoS Attacked Networks,”, Journal
- Anjali Sardana and R. C. Joshi, ”Dual-Level Defense For Networks Under DDoS
- Anjali Sardana and R. C. Joshi, ”Dual-Level Attack Detection, Characterization
  and Response for Networks under DDoS Attacks,”, International Journal of Mobile
- Anjali Sardana and R. C. Joshi, ”Dual-Level Attack Detection and
  Characterization for Networks under DDoS,”, International Conference on Availability,
- Wenbo Mao, ”Modern Cryptography: Theory and Practice,”, Pearson
Proxy Base Station based Authentication Protocol for Broadband Wireless Network


Index Terms

Computer Science Wireless
Keywords
WiMAX  Authentication  Proxy  Base station  protocol  Privacy and key management